Theoretical Computer Science 52 (1987) 239–249
North-Holland

MODELS OF LOWER-BOUNDS PROOFS*

R.G. NIGMATULLIN
Theoretical Cybernetics Chair, Kazan State University, 420 008 Kazan, U.S.S.R.

Communicated by G. Mirkowska
Received August 1986
Revised January 1987

Abstract. Two models of proofs of lower bounds on the complexity are introduced. They have very wide applicability. The purpose of the models is to explain the difficulties of establishing high lower bounds on the complexity.

1. Introduction

The lower-bounds problem is one of the most difficult open problems in mathematics. It consists in proving high (e.g., superpolynomial) effective lower bounds on the complexity of functions or languages. What is meant here by the word 'effective'? To answer this question, recall that Shannon's counting argument and diagonalization do enable one to produce very high (e.g., exponential) lower bounds. But these methods merely prove the existence of functions or languages of high complexity. They are not applicable to any explicit function or language. So we call lower bounds provided by similar methods *noneffective* ones.

Among theoretical computer scientists there wanders a conjecture asserting that the lower-bounds problem cannot be settled by effective methods, i.e., a hypothesis on the negative solution of the lower-bounds problem. Confirmation of this conjecture needs a more accurate notion of effectiveness. One can make the definition of effective lower bounds more precise in various ways.

One way of making this definition more precise is to associate the effectiveness with the algebraic complexity of languages. Such an approach was proposed in [10]. In the most refined form it suggests to prove high lower bounds for languages from NP, closing up with the well known problem P=?NP. Since the last problem has no fruitful approaches, the first way is not likely to be worth-while.

* The paper is based on the text of two lectures given by the author at the International Banach Mathematical Center (Warsaw, November 1985). Russian text of the lectures is submitted to the Banach Center Publications.